D10
31992

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
23 May 2002 (23.05.2002)

PCT

(10) International Publication Number
WO 02/41602 A1

(51) International Patent Classification⁷: H04L 29/08, 9/30

(21) International Application Number: PCT/FI01/00985

(22) International Filing Date: 13 November 2001 (13.11.2001)

(25) Filing Language: Finnish

(26) Publication Language: English

(30) Priority Data:
20002508 15 November 2000 (15.11.2000) FI

(71) Applicant *(for all designated States except US)*: SONERA SMARTTRUST OY [FI/FI]; Elimäenkatu 17-19, FIN-00510 Helsinki (FI).

(72) Inventors; and
(75) Inventors/Applicants *(for US only)*: HEINONEN, Petteri [FI/FI]; Postipuuntie 12 D 52, FIN-02600 Espoo (FI). OTRANEN, Jari [FI/FI]; Tähkäkuja 5 F 80, FIN-01370 Vantaa (FI). HÄMÄLÄINEN, Antti, P., J. [FI/FI]; Piennar 2, FIN-00680 Helsinki (FI). HARJULA, Jari [FI/FI]; c/o Sonera Smarttrust Oy, Elimäenkatu 17-19, FIN-00510 Helsinki (FI).

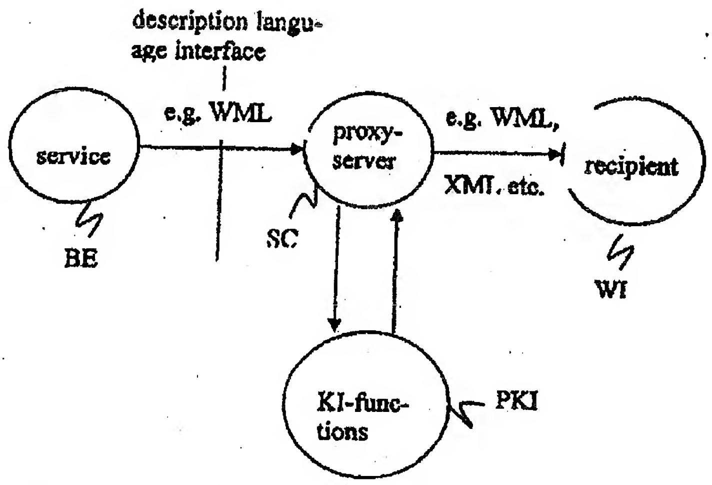
(74) Agent: PAPULA OY; P.O. Box 981, Fredrikinkatu 61 A, FIN-00101 Helsinki (FI).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AT (utility model), AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, CZ (utility model), DE, DE (utility model), DK, DK (utility model), DM, DZ, EC, EE, EE (utility model), ES, FI, FI (utility model), GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK, SK (utility model), SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF,

[Continued on next page]

(54) Title: METHOD FOR FORMING AN INTERFACE



(57) Abstract: The invention is concerned with a method for the forming of a terminal independent interface for security functions between a service and a receiver using standardized page description language. In accordance with the invention the necessary function call requests concerned with the security measures are encapsulated in the service into a document in accordance with the standardized page description language; the identification data of the recipient is included into the document; the document is mediated to the proxy-server; said functions are called with the proxy-server for the realisation of said security measures; the protocol used by the recipient is checked with the proxy-server; the document in accordance with the standardized page description language handled with the security measures, received from the service, is mediated with the proxy-server to the recipient using a transmission protocol understood by the recipient.

CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:

— *with international search report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

METHOD FOR FORMING AN INTERFACE

TECHNICAL FIELD

The presented invention is concerned with telecommunications technology. The invention especially targets on a method for the forming of a terminal independent interface for security functions between a service and its recipient while using standardized page description language.

BACKGROUND OF THE INVENTION

The use of the wireless application protocol (WAP, Wireless Application Protocol) is becoming more common in solutions where a connection between mobile terminals, as a mobile phone, and internet applications, for instance e-mail, the WWW (World Wide Web) and newsgroups, is needed. The wireless application protocol offers an architecture which fits mobile phones, the browser programs of mobile phones and the WWW into a working wholeness. The HTML-language (Hyper Text Markup Language) used in the WWW can, when necessary, be transformed into WML (Wireless Markup Language) which has been developed for the wireless environment, when data is transferred to mobile stations. At present the description language of the WAP-standard is the WML-language, but also any other description language in accordance with the coming WAP-standard can be comprised as the language.

The wireless application protocol comprises five layers: the wireless application environment (WAE, Wireless Application Environment), the wireless session layer (WSL, Wireless Session Layer), the wireless transaction layer (WTL, Wireless Transaction Layer), the wireless transport layer security layer (WTLS, Wireless Transport Layer Security) and the wireless transfer layer (WDP, Wireless Datagram Layer). With wireless application environment it is meant for instance WTA (WTA, Wireless Telephone Application) or any other suitable environment. There is furthermore a system dependant layer as the lowest layers , which defines the way in which the information is transported inside the system in question. At present the last accepted WAP-specification version number is 1.3.

The especial purpose of the WAP-architecture is to make it possible to use, among others, services in the internet on the mobile terminals, the data handling ability, screen size or memory capacity of which is small or limited. Terminals like the ones described are for instance mobile stations and PDAs (PDA, Personal Digital Assistant). The WAP-specification does not take a stand on how the air interface is realized. This makes it possible for several different operators, terminal manufacturers and program manufacturers to benefit from the possibilities that the standard brings with it.

At present the problem is how to use the standardized page description language, for instance WML, for the making of an encryption and a digital signature without restricting to a certain encryption or signature method or terminal. Furthermore, a problem is that for instance the WTLS-encryption handling the encryption of data in the WAP-protocol is not a pure end-to-end encryption; the encryption can be decrypted in between. The contents can be accessed and thus the risk is that it can be altered. Thus, the confidence in the data contents and its integrity is lost.

A certain solution is to use manufacturer specific page description languages, for example a manufacturer specific WML-language, which still is not in accordance with a standard. This leads to that all the components in the network and the terminal at the end of the chain do not understand the manufacturer specific page description language.

Another solution is to use script language, for example WMLScript, but the problem with this alternative is the lack of functions necessary for encryption and signature. Furthermore, the inconvenience with using the script-language is that the terminals browser program does not necessarily support the use of the script language.

In addition, a situation where new functions are wanted to be added to the service becomes troublesome. The producer of the service has to translate the program after each change. The changes made are often dependent on the terminal, so different changes have to be made on different programs.

OBJECT OF THE INVENTION

The purpose of the invention is to remove or at least significantly alleviate the disadvantages mentioned above. Especially, the invention is concerned with a new kind of method, with which a terminal-independent interface can be offered to the service provider, through which interface functions concerned with the security measures can be called.

SUMMARY OF THE INVENTION

The present invention is concerned with a method for the forming of a terminal-independent interface for security functions between the service and the recipient while using a standardized page description language. With standardized page description language it is referred to for example the WML-language.

In the method in accordance with the invention the function call requests concerned with the security measures are encapsulated in the service into a document in accordance with the standardized page description language. If the page description language is WML, the do-element with a type-attribute is used, with which do-type the security measures to be performed to the proxy-server are defined.

With service it is referred to a service offered by a service provider, where security measures are needed. Security measures are for instance a digital signature, the verification of a digital signature, the encryption of data, the decryption of data and so forth. A service provider is for instance a bank, a credit card company, an Internet shop etc. A service is therefore for instance a bank service that demands security measures. The service adds the identity data referring to the final recipient of the document into the document formed by the service. The service transmits the document to the proxy-server. Said functions are called with the proxy-server for the realisation of said security measures. The function calls can be realized on the proxy-server itself or they can be transmitted to a separate PKI-server, which takes care of the security measures. In said security measures a symmetric or an asymmetric method is used for the signature and/or encryption. Methods like these are for instance 3DES (3DES, Triple Data Encryption Standard) and RSA (RSA, Rivest Shamir Adleman).

The protocol used by the recipient is checked with the proxy-server. The document in accordance with the standardized page description language handled with the security measures received from the service is transmitted with the proxy-server to the recipient with the transmission protocol understood by the recipient. If the page description language is WML, the document in accordance with the standardized WML-language is, if necessary, changed to a manufacturer specific WML-language, XML-language (XML, eXtended Markup Language) or to another form understood by the recipient. If the recipient cannot interpret the received document, it can be ignored.

The sending of information between the service and the recipient can be activated in different ways. In a certain case the recipient first sends a request, to which the service responds. In another case the service sends information to the recipient with a push-method without a request from the recipient. In the before mentioned case the proxy-server checks the protocol used by the recipient in the request and transmits the document, received from the service as a response to the request, in accordance with the standardized page description language which has been handled with security measures to the recipient in accordance with the protocol used by the recipient.

In the latter case the recipient does not first transmit a service request to the service, but the service uses the push-function. In this case the service sends the document to be sent to the recipient to the proxy-server and at the same time identifies the recipient, to which the proxy-server later transmits the document handled with the security measures. The identification data is for instance a network identity or an MSISDN-number (MSISDN, Mobile Subscriber ISDN). A network identity is an unambiguous user specific identifier, to which signature and encryption keys have been attached during the creation of it. Corresponding data pairs are maintained on the proxy-server, with which the recipient's identification data and transmission protocol are tied together. The proxy-server can choose the right transmission protocol on the basis of the identification data connected with the recipient received from the service.

Because of the present invention the faction offering services to a fixed line or wireless terminal which demand security measures does not need to care about the recipient's terminal or its attributes. An interface is offered to the faction offering a service, through which it calls the necessary security measures in a terminal independent way. The security function requests are always sent from the service in accordance with the standardized page description language. Because of the interface the faction offering services does not need to update its software with terminal specific changes.

Because of the invention the functions concerned with the digital signature and encryption can be taken into widespread use regardless of page description language.

BRIEF DESCRIPTION OF THE DRAWINGS

The accompanying drawings, which are included to provide a further understanding of the invention and constitute a part of this specification, illustrate embodiments of the invention and together with the description help to explain the principles of the invention. In the drawings:

figure 1 presents the functioning of the method in accordance with the presented invention, and

figure 2 presents a certain advantageous system, in which the method in accordance with the invention can be realized.

DETAILED DESCRIPTION OF THE INVENTION

Figure 1 presents the functionality of the method in accordance with the invention. The method in accordance with the invention is concerned with the forming of a terminal independent interface for the security measures between the service and the recipient while using standardized page description language. Security measures are for instance a digital signature, the verification of a signature, the encryption of data, the decryption of data etc. With standardized page description language it is referred to for instance WML-language.

In accordance with block 10 the necessary function requests concerned with the security measures are encapsulated into the document in accordance with the standardized page description language. The service can send information to the recipient with the push-method without an actual service request. In the second alternative the recipient has, before block 10, sent a service request for the receiving of information. In this case the service request made by the recipient contains the identification data of the recipient, on the basis of which the service can send the response to the right recipient.

The service attaches the identification data of the recipient into the document, block 11. In accordance with block 12 the document is transmitted to the proxy-server. With the proxy-server said functions are called for the realisation of said security measures, block 13. Said functions can be called in the proxy-server or in a separate PKI-server (PKI, Public Key Infrastructure). A symmetric or an asymmetric method is used for the signature and/or encryption concerned with the security measures.

In accordance with block 14 the protocol used by the recipient is checked with the proxy-server. The proxy-server maintains corresponding data pairs, with which the identification data and transmission protocol of the recipient are tied together. With the identification data it is for instance referred to a network identity or an MSISDN-number. The network identity is an unambiguous user specific identity, to which has been attached signature and encryption keys during its creation. The proxy-server searches identification data of the recipient defined by the service and can thereby choose the right transmission protocol. The proxy-server transmits the document, in accordance with the page description language, handled with the security measures to the recipient using the transmission protocol understood by the recipient, block 15. If the recipient cannot interpret the received document, it can be ignored.

Because of the invention the security function requests are always sent using the standardized page description language. Because of the interface the faction offering services does not need to update its software with terminal specific changes.

The example in accordance with figure 2 consists of the service BE, the proxy-server SC, the PKI-server PKI and the recipient WIB. With service BE it is referred to for instance a bank's, a credit institution's or an online trader's service in which security measures are taken advantage of. Security measures are for instance a digital signature, the verification of a signature, the encryption of data, the decryption of data etc. The proxy-server can execute the demanded security functions itself or send the function requests concerned with the security measures to the PKI-server PKI.

In the example in accordance with figure 2 information between the service BE and the proxy-server SC is transmitted in accordance with the standardized WML-description language. The information between the proxy-server SC and the recipient WIB is transmitted in accordance with WML-language, manufacturer specific WML-language, XML-language or in accordance with another form of data transfer suited to the purpose. With recipient the WIB it is advantageously referred to a terminal, a browser program of a terminal, software of a terminal or other, with which the information sent from the proxy-server SC can be handled.

In the following the functioning of the example in accordance with figure 2 is explained more specifically. Even though it is presented in the following that the page description language between the service and the proxy-server is WML, it can be any other language suited for the purpose, for example XML, HTML (Hyper Text Markup Language), HDML (HDML, Handheld device Markup Language) etc. The starting point of the invention is to function in such a way that the data traffic between the service BE and the proxy-server SC is in accordance with standardized page description language.

In this example the do-element is used with the type-attribute. The type-attribute gives the receiving party a reference on how the user of the do-element wants it to be used. Most of the type-attributes are reserved, but experimental and manufacturer specific ones have been defined into the language. These attributes can be used to broaden the WML-language, but still simultaneously preserve the definitions of the WML-specifications. When manufacturer specific type-attributes are used, the proxy-server SC can interpret the requests concerned with the security measures from a standard according WML-document, whereas standardized WAP-clients ignore this information.

The interface and the way in which the service BE sends security function requests to the proxy-server is described in the following. A signature request has been presented in the following.

```
<do type="vnd.smarttrust.sign" label="SIGN" optional=
"true">
   <refresh>
      <setvar name="signParam" value="foo"/>
      <setvarname="transID"value="TRANSACTION_ID"/>
```

```
            <setvar name="options" value="OPTIONS"/>
            <setvar name="keyIdType" value="12345"/>
            <setvar name="keyId" value="KEY_ID"/>
            <setvar name="userIDType" value="12345"/>
            <setvar name="userID" value="USERID"/>
            <setvar name="modifiable" value="true|false"/>
        </refresh>
    </do>
```

The **label**-attribute in the do-element has at most a length of six characters and it only serves a purpose as a giver of information. The **optional**-attribute in the do-element makes it possible for the recipient WIB to ignore the used do-element.

Of the columns appearing in the table WIG refers to the realisation way of the invention and WAP to the realisation way of the nearest technical standard. In the columns ""M"" means mandatory and "O" optional.

Attribute	**Type**	**Explanation**	**WIG**	**WAP**

UserID-Type	String (Integer Value)	Defines the user identification type which the service BE uses, with which it is placed abreast with the NID/MSISDN used by the proxy-server SC.
		NID = 1
		MSISDN = 2
		BESPECIFIC = 3
			M	M

UserID	String	Identifies the user.	M	M
Sign Param	String	The name of the URL-parameter which is returned in the HTTP GET-	M	M

		request, signed by the recipient WIB.		
TransID	String	An unambiguous transaction mark.	M	M
Options	Integer	In use only in WAP-client programs.	O	M
KeyID Type	String (Integer Value)	In use only in WAP-client programs	O	M
KeyID	String	In use only in WAP-client programs.	O	M
Modifiable	String	Defines if the signed parameter is static ("false") or dynamic ("true").	O	O

The interface and the way in which the service BE sends security function requests to the proxy-server is described in the following. Another way to make a signature request is presented in the following. The MAC (ISO 9797) method is used. On the basis of the request the fed information is signed with the 3DES-method (3DES, Triple Data Encryption Standard) in an external CBC-mode (CBC, Cell Block Cipher) using two keys.

```
<do type=″vnd.smarttrust.kmac″ label=″KMAC″ optional=
″true″>
    <refresh>
       <setvar name=″signParam″ value=″foo″/>
       <setvar name=″transID″ value=″TRANSACTION_ID″/>
       <setvar name=″userIDType″ value=″12345″/>
       <setvar name=″userID″ value=″USERID″/>
       <setvar name=″modifiable″ value=″true|false″/>
    </refresh>
</do>
```

The label-attribute in the do-element has at most a length of six characters and it only serves a purpose as a giver of information. The optional-attribute in the do-element makes it possible for the recipient WIB to ignore the used do-element.

Attribute	Type	Explanation	WIG	WAP

UserID-Type	String (Integer Value)	Defines the user identification type which the service BE uses, with which it is placed abreast with the NID/MSISDN used by the proxy-server SC.
		NID = 1
		MSISDN = 2
		BESPECIFIC = 3
			M	M

UserID	String	Identifies the user.	M	M
Sign Param	String	The name of the URL-parameter which is returned in the HTTP GET-request, signed by the recipient WIB.	M	M
TransID	String	An unambiguous transaction mark.	M	M
Modifiable	String	Defines if the signed parameter is static ("false") or dynamic ("true").	O	O

The interface and the way in which the service BE sends security function requests to the proxy-server is described in the following. An encryption request is presented in the following. On the basis of the request the input information is encrypted using the 3DES-method in an external CBC-mode using two keys.

```
<do type="vnd.smarttrust.encrypt" label="ENCR" optional="true">
    <refresh>
       <setvar name="encryptParam" value="foo"/>
       <setvar name="userIDType" value="12345"/>
       <setvar name="userID" value="USERID"/>
    </refresh>
</do>
```

The "X" in the table means that the nearest technical standard WAP does not at present support this function.

Attribute	**Type**	**Explanation**	**WIG**	**WAP**
Encrypt Param	String	Character line which contains the name of the variable which the recipient WIB encrypts.	M	X
UserID-Type	String (Integer Value)	Defines the user identification type which the service BE uses, with which it is placed abreast with the NID/MSISDN used by the proxy-server SC. NID = 1	M	X

		MSISDN = 2
		BESPECIFIC = 3		

UserID	String	Identifies the user.	M	X

The interface and the way which the service BE sends security function requests to the proxy-server is described in the following. A decryption request is presented in the following. On the basis of the request the encryption is decrypted with the 3DES-method in an external CBC-mode using two keys.

```
<do type="vnd.smarttrust.decrypt" label="DECR" optional="true">
    <refresh>
       <setvar name="stringToDecrypt" value="plain"/>
       <setvar name="decryptedString" value="foo"/>
       <setvar name="userIDType" value="12345"/>
       <setvar name="userID" value="USERID"/>
    </refresh>
</do>
```

Attribute	Type	Explanation	WIG	WAP
StringTo-Decrypt	String	Information which is encrypted using the proxy-server and which the recipient WIB decrypts.	M	X
Decrypted String	String	A variable, to where the information which has been decrypted by the recipient WIB to plain text is set.	M	X

UserID-Type	String (Integer Value)	Defines the user identification type which the service BE uses, with which it is placed abreast with the NID/MSISDN used by the proxy-server SC.
		NID = 1
		MSISDN = 2
		BESPECIFIC = 3
			M	X

UserID	String	Identifies the user	M	X

Furthermore, the interface between the service BE and the proxy-server SC is described in the following. When implementing security measures it is possible to take advantage of the first function call's output as the argument for the second function call. Such a situation can arise in for instance the following situations.

1. The service BE sends information, which is encrypted using the proxy-server SC and which the recipient WIB decrypts. The value of the decrypted variable can furthermore be for instance shown to the user or be

used as an argument for an encryption service.

2. The information is signed before performing the encryption.

In the following it is exemplary presented, how the data in the contract-variable is signed using the do-type and then how the signed data in the contract-variable is encrypted using the do-type (contract consists of all the variables prefix, amount and suffix).

```
<do type=”vnd.smarttrust.sign” optional=”true”>
    <refresh>
       <setvar name=”modifiable” value=”true”/>
       <setvar name=”signedParam” value=”contract”/>
       <setvar name=”userIDType” value=”3”/>
       <setvar name=”userID” value=”test user”/>
    </refresh>
</do>

<do type=”vnd.smarttrust.encrypt” optional=”true”>
    <refresh>
       <setvar name=”encryptParam” value=”contract”/>
       <setvar name=”userIDType” value=”3”/>
       <setvar name=”userID” value=”test user”/>
    </refresh>
</do>

<p>
<anchor>
<go
href=”http://www.backend.com/file?contract=$(prefix)$(
amount)$(suffix)”/>
</anchor>
</p>
```

In the following it is exemplary presented, how the proxy-server SC can alter the presentation form of the generic do-type in order to correspond to the receiving terminal while using security functions.

The recipient WIB requests sensitive information from the service BE. The service BE transmits the following WML-card as a response to the request to the proxy-server SC.

```
<wml>
  <card>
    <do type="vnd.smarttrust.decrypt" optional="true">
      <refresh>
        <setvar name="stringToDecrypt" value="account
balance : -100 FIM"/>
        <setvar name="decryptedString" value="output"/>
        <setvar name="userIDType" value="3"/>
        <setvar name="userID" value="test user"/>
      </refresh>
    </do>
    <p>
    $(output) <!--displays the data without padding
bytes -->
    </p>
  </card>
</wml>
```

The proxy-server SC encrypts the character line "account balance: -100FIM" and transmits the information to the recipient WIB. The recipient WIB decrypts the encryption and stores the data into the output-variable, which value can be for instance shown to the user.

It is described as an example in the following, how the recipient WIB sends confidential information to the service BE. The data to be sent is for instance a password. The user enters the password to a given input field. The recipient WIB encrypts the value of the pwd-variable (password) and sends it to the proxy-server SC.

```
<wml>
  <card>
    <p>
    <input    title="enter    password"    type="text"
name="password"/>
    </p>
    <do type="vnd.smarttrust.encrypt" optional="true">
      <refresh>
         <setvar name="encryptParam" value="pwd"/>
         <setvar name="userIDType" value="3"/>
         <setvar name="userID" value="test user"/>
      </refresh>
    </do>
    <p>
    <anchor>
      <go href="http://www.back-end.com/file?pwd=$(pas
sword)"/>
    </anchor>
    </p>
  </card>
</wml>
```

The proxy-server SC decrypts the encryption of the pwd-variable and sends an HTTP GET-request to the service, which consists of the stored plain text of the pwd-variable.

```
GET /file?pwd="password entered" HTTP /1.1
```

It is described as an example in the following, how the recipient WIB signs and encrypts the received payment request or contract received from the service BE. The recipient WIB uses the MAC-method for the signature. The example consists of three phases:

1. Encrypted data is sent to the recipient WIB, that consists of a frame agreement: "prefix" and "suffix". These can be any static data, for instance prefilled fields.
2. The "contract"-variable consists of the following data: "prefix" + the input of the user + "suffix". The data said above is signed after the PIN-inquiry confirmation (PIN, Personal Identification Number).
3. The data in the "contract"-variable said above is encrypted.

```
<wml>
  <card>
    <do type="vnd.smarttrust.decrypt" optional="true">
      <refresh>
         <setvar name="stringToDecrypt" value="I wish to
buy"/>
         <setvar name="decryptedString" value="prefix"/>
         <setvar name="userIDType" value="3"/>
         <setvar name="userID" value="test user"/>
      </refresh>
    </do>

    <do type="vnd.smarttrust.decrypt" optional="true">
      <refresh>
         <setvar name="stringToDecrypt" value="Pokemon
Figures"/>
         <setvar name="decryptedString" value="suffix"/>
         <setvar name="userIDType" value="3"/>
         <setvar name="userID" value="test user"/>
      </refresh>
    </do>

    <p>
    <input type="text" name="amount"/>
    </p>

    <do type="vnd.smarttrust.kmac" optional="true">
      <refresh>
         <setvar name="modifiable" value="true"/>
         <setvar name="signedParam" value="contract"/>
         <setvar name="userIDType" value="3"/>
         <setvar name="userID" value="test user"/>
      </refresh>
    </do>

    <do type="vnd.smarttrust.encrypt" optional="true">
      <refresh>
         <setvar name="encryptParam" value="contract"/>
         <setvar name="userIDType" value="3"/>
         <setvar name="userID" value="test user"/>
      </refresh>
    </do>

    <p>
    <anchor>
    <go href="http://www.back-end.com/file?contract=$(
prefix)$(amount)$(suffix)"/>
    </anchor>
    </p>
  </card>
</wml>
```

The proxy-server SC decrypts the encryption and verifies the signature. Thereafter the proxy-server sends an HTTP GET-request to the service BE.

```
GET /file?contract=" I wish to buy X Pokemon figures"&KMAC_FIELDS="contract" HTTP /1.1
```

The request furthermore consists of the KMAC_FIELDS-parameter, which indicates the verified parameters.

It is described as an example in the following, how the recipient WIB signs and encrypts the payment request or contract, received from the service BE. In this example the recipient WIB uses an RSA-signature. The example consists of three phases:

1. Encrypted data is sent to the recipient WIB, that consists of a frame agreement: "prefix" and "suffix". These can be any static data, for instance prefilled fields.
2. The "contract"-variable consists of the following data: "prefix" + the input of the user + "suffix". The data said above is signed after the PIN-inquiry confirmation (PIN, Personal Identification Number).
3. The data in the "contract"-variable said above is encrypted.

```
<wml>
  <card>
    <do type="vnd.smarttrust.decrypt" optional="true">
      <refresh>
          <setvar name="stringToDecrypt" value="I wish
to buy"/>
          <setvar name="decryptedString" value="prefix"/>
          <setvar name="userIDType" value="3"/>
          <setvar name="userID" value="test user"/>
      </refresh>
    </do>

    <do type="vnd.smarttrust.decrypt" optional="true">
      <refresh>
          <setvar name="stringToDecrypt" value="Pokemon
figures"/>
          <setvar name="decryptedString" value="suffix"/>
```

```
     <setvar name="userIDType" value="3"/>
     <setvar name="userID" value="test user"/>
   </refresh>
  </do>

  <p>
  <input type="text" name="amount"/>
  </p>

  <do type="vnd.smarttrust.sign" optional="true">
   <refresh>
     <setvar name="modifiable" value="true"/>
     <setvar name="signedParam" value="contract"/>
     <setvar name="userIDType" value="3"/>
     <setvar name="userID" value="test user"/>
   </refresh>
  </do>

  <do type="vnd.smarttrust.encrypt" optional="true">
   <refresh>
     <setvar name="encryptParam" value="contract"/>
     <setvar name="userIDType" value="3"/>
     <setvar name="userID" value="test user"/>
   </refresh>
  </do>

  <p>
  <anchor>
  <go  href="http://www.back-end.com/file?contract=$
(prefix)$(amount)$(suffix)"/>
  </anchor>
  </p>
 </card>
</wml>
```

The proxy-server SC decrypts the encryption and verifies the signature. Thereafter the proxy-server sends an HTTP GET-request to the service BE.

GET /file?contract=" I wish to buy X Pokemon figures"&NR_FIELDS="contract" HTTP /1.1

The request furthermore consists of the NR_FIELDS-parameter, which indicates the verified parameters.

In a certain application in accordance with figure 2 the <do type> -structure is not transmitted as such to the recipient. The <do type> -structure can be replaced with a manufacturer specific WMLScript plugin function call. The function call referring to the signature is for instance of the form http://manufacturer. com (sig, x, x). If the recipient's terminal is a computer the signature invitation in accordance with the <do type> -structure is changed for instance into the XML-signature request from.

Because of the invention the functions concerned with the digital signature and encryption can be taken into widespread use regardless of page description language used. With the present invention a service calls the necessary security measures in a terminal independent way through an interface offered to the service. The service does not need to care about the type of the terminal of the recipient.

The invention is not limited to solely concern the application examples presented above, other variations are possible while staying within the inventive idea defined by the claims.

CLAIMS

1. A method for the forming of a terminal independent interface for security functions between a service and a receiver using standardized page description language,

characterized in that the method comprises the following steps:

a) encapsulating in the service the necessary function call requests concerned with the security measures into a document in accordance with the standardized page description language;

b) including the identification data of the recipient into the document;

c) transmitting the document to the proxy-server;

d) calling said functions with the proxy-server for the realisation of said security measures; and

e) checking the protocol used by the recipient with the proxy-server;

f) transmitting the document in accordance with the standardized page description language handled with the security measures, received from the service, with the proxy-server to the recipient using a transmission protocol understood by the recipient.

2. The method according to claim 1, characterized in that

g) the received document is left unnoticed if the recipient cannot interpret the document.

3. The method according to claim 1, characterized in that if the page description language is WML, then in step a):

using a do-element with a manufacturer specific type-attribute, with which the do-type defines the security measures to be performed on the proxy-server.

4. The method according to claim 1, characterized in that if the page description language is WML, then in connection with step f):

changing the document in accordance with the standardized WML-language to a manufacturer specific WML-language, XML-language or to some other form understood by the recipient.

5. The method according to claim 1, characterized in that in the signature and/or encryption, in said security measures, a symmetric or an asymmetric method is used.

6. The method according to claim 1, characterized in that in step d):

calling said functions with the proxy-server from the PKI-server for the realisation of said security measures.

7. The method according to claim 1, characterized in that before step a):

sending a service request from the recipient to the service.

8. The method according to claim 7, characterized in that the service request comprises the identification data of the sender of the service request.

9. The method according to claim 1, characterized in that corresponding data pairs are upheld on the proxy-server, with which the recipient's identification data and transmission protocol are tied together.

10. The method according to claim 1 or 9, characterized in that the recipient's identification data is a network identity.

11. The method according to claim 1 or 9, characterized in that the recipient's identification data is an MSISDN-number.

12. The method according to claim 1 or 9, characterized in that in connection with step d):

checking the transmission protocol used by the recipient with the proxy-server on the basis of the recipient's identification data.

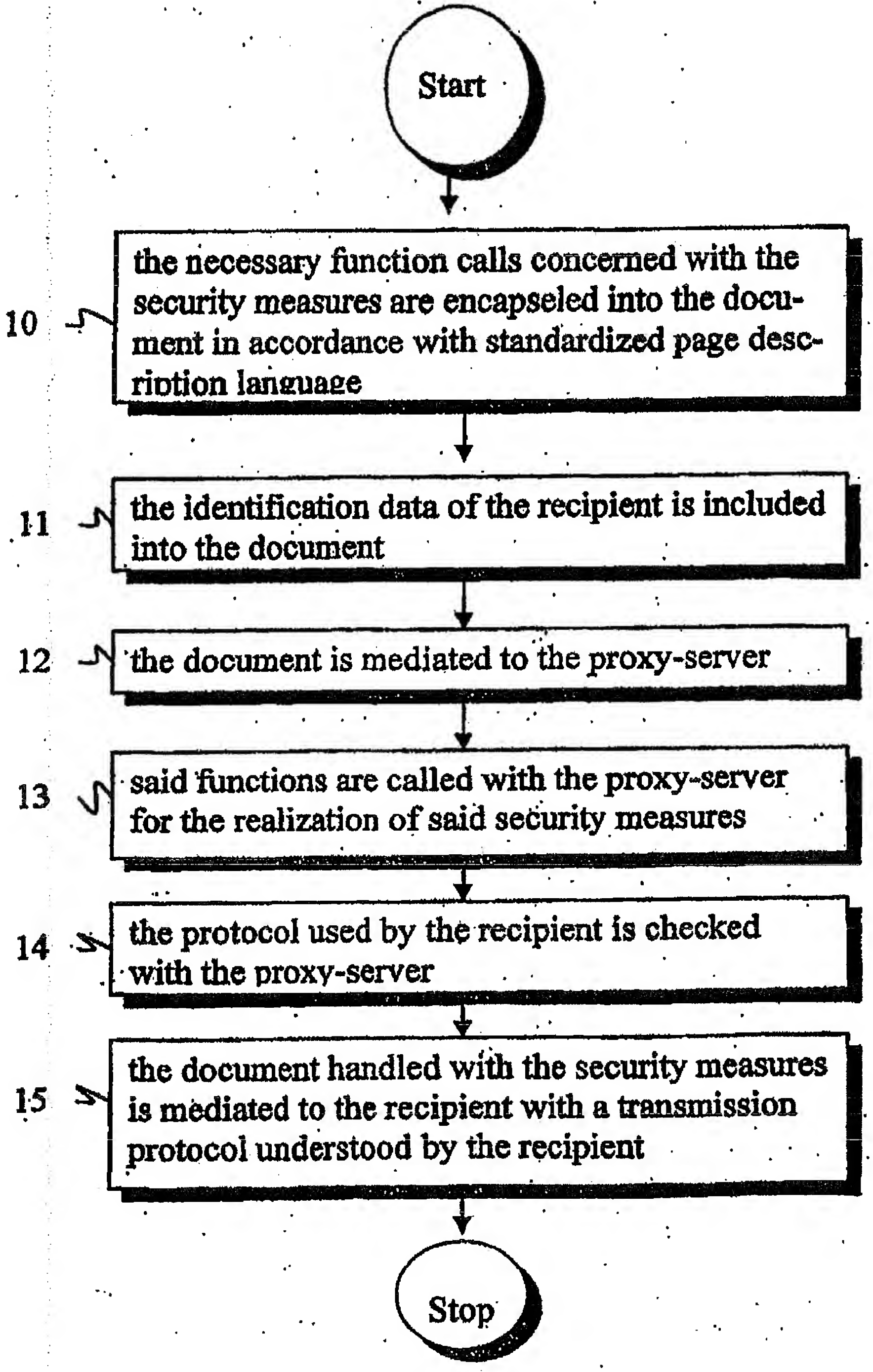

Start
10
the necessary function calls concerned with the security measures are encapseled into the document in accordance with standardized page description language
11
the identification data of the recipient is included into the document
12
the document is mediated to the proxy-server
13
said functions are called with the proxy-server for the realization of said security measures
14
the protocol used by the recipient is checked with the proxy-server
15
the document handled with the security measures is mediated to the recipient with a transmission protocol understood by the recipient
Stop

Fig. 1

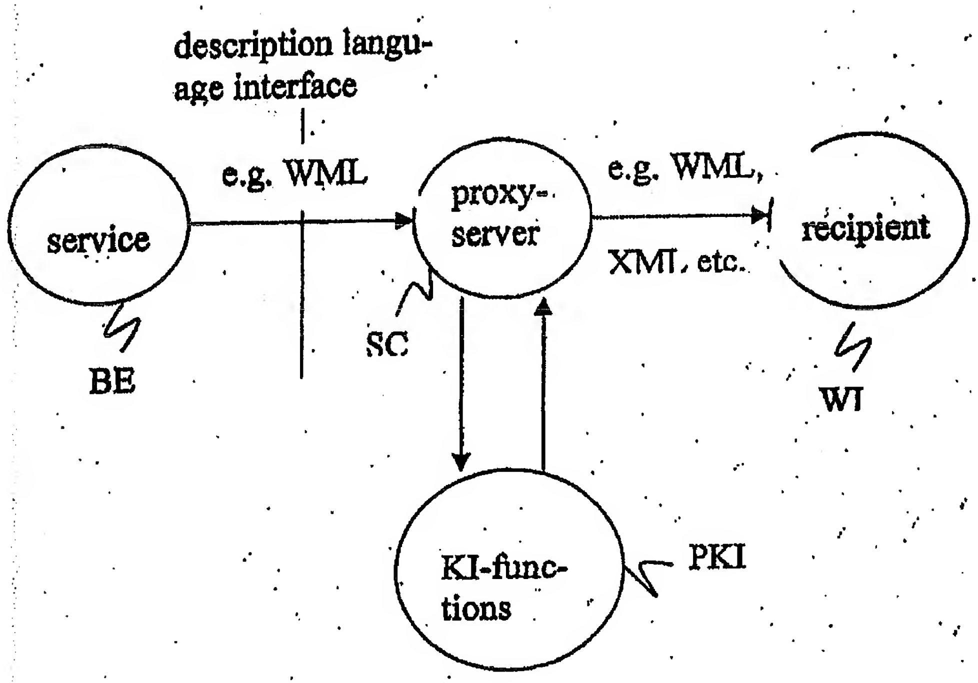

description language interface
e.g. WML
service
BE
proxy-server
SC
e.g. WML, XML etc.
recipient
WI
KI-functions
PKI

Fig. 2

INTERNATIONAL SEARCH REPORT

International application No.
PCT/FI 01/00985

A. CLASSIFICATION OF SUBJECT MATTER

IPC7: H04L 29/08, H04L 9/30

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC7: H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

SE,DK,FI,NO classes as above

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

EPO-INTERNAL, WPI DATA, PAJ

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	WO 0059149 A1 (MOTOROLA INC.), 5 October 2000 (05.10.00), page 1, line 25 - page 2, line 11; page 3, line 24 - page 6, line 22; page 9, line 27 - page 10, line 13 --	1
Y	Information Security Magazine, October 2000 "WIRELESS SECURITY: LOCKING DOWN THE..." Edmund X. Dejesus sections "Mobile Pkl", "Pkl Alternative" --	1
P,Y	WO 0118716 A1 (BRANDENBURG, JACKSON ET AL), 15 March 2001 (15.03.01), page 2, line 9 - page 3, line 31 --	1

☒ Further documents are listed in the continuation of Box C.   ☒ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance: the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance: the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search 28 February 2002	Date of mailing of the international search report 01 -03- 2002
Name and mailing address of the ISA/ Swedish Patent Office Box 5055, S-102 42 STOCKHOLM Facsimile No. +46 8 666 02 86	Authorized officer Marianne Norrgren/mj Telephone No. +46 8 782 25 00

INTERNATIONAL SEARCH REPORT

International application No.
PCT/FI 01/00985

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
E,X	2001, SmartTrust "White Paper" "WAP it and WIBbit it good!" Sten Lannerström PA4, January 10, 2002 Doc.no. SPN 01:0033 Http://www.smarttrust.com/ --	1-12
A	Prasad, V. et al, "Scalable policy driven and general purpose public key infrastructure (PKI)" Computer Security Applications, 2000. ACSAC Annual Conference, December 2000, Pages 138-147 ISBN: 0-7695-0859-6 -- --------	1-12

INTERNATIONAL SEARCH REPORT

Information on patent family members

28/01/02

International application No.
PCT/FI 01/00985

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 0059149 A1	05/10/00	AU 3498600 A EP 1166490 A US 6223291 B	16/10/00 02/01/02 24/04/01
WO 0118716 A1	15/03/01	AU 7123900 A	10/04/01